**Amendments to the Specification**:

Page 1

Please substitute the following paragraph for the paragraph beginning at line 5:

This application claims priority of U. S. provisional Application S. N. 60/248,906, filed November 15, 2000, and assigned to the assignee of the present application, as does concurrently filed related application 09/973,769 (Docket Number ~~FS-00510~~FS-00509 ~~(02890038AA)~~) both of which are hereby fully incorporated by reference.

Page 12

Please substitute the following paragraph for the paragraph beginning at line 12:

Functionally, it should be appreciated that the processor arrangement 113 can implement any number of objects for fault or intrusion detection and which may be of any arbitrary design, including a number of algorithms which are commercially available for the purpose. Results of the execution of these objects can be communicated over normal network links to other nodes and used by manager objects to exercise any desired control over the locking devices, to implement any desired security policy (e.g. mandatory access control (MAC), Discretionary~~Discretionalry~~ access control (DAC), and the like) and/or to log any desired information concerning the status or operations of any node through other managed objects at each node. More generally, managed objects include network interface managed objects, intrusion detection managed objects and network service managed objects.

Page 12

Please substitute the following paragraph for the paragraph beginning at line 33:

All of these communications are preferably performed in a user transparent fashion at high bit rates and encrypted in accordance with any desired encryption algorithm (DES, DES-3 or Type 1 algorithms implemented in hardware for highest speed being preferred) which may also be altered and keys arbitrarily exchanged and altered by the same type of communications which are entirely transparent to all users and may be made arbitrarily difficult to intercept by any of a number of known techniques which will be evident to those skilled in the art. Further, each transmission or group of transmissions (for~~for~~ a given user) may be supplied with identification information (e.g. in the form of a stamp or the like) by processor 113, even if the user is not identified and any desired tracking or logging information may be transmitted to other nodes for error recovery and determination of the source of any detected potential attack as well as continuous monitoring and authentication of the source node for all communications, potentially to the data packet level.

Page 14

Please substitute the following paragraph for the paragraph beginning at line 31:

For example, a communication link depicted by dashed line 430 could be used as a communication link through tier 405 with tier 407 above tier 403 or to place a node of tier 403 hierarchically above tier 405~~407~~. Nevertheless, an organization containing communications links such as 430 may engender unjustified complexity although some

advantages may accrue such as establishing further redundant communication paths and/or avoiding a top level of the hierarchy which might be an excessively attractive target for attack.

Page 15

Please substitute the following paragraph for the paragraph beginning at line 2:

It should be noted that the network shown in Figure 2~~Figure 4~~ (without link 430) provides redundant communication links between all nodes of the network even though there are no links between nodes of the same tier, as is also preferred for practice of the invention. (In this regard, however, it should be recognized that the assignment of any given tier to any given node is arbitrary.) For example, node 440 can communicate with node 450 over communication links 427, 423, 419 and 421; 427, 415, 418 and 425; or 427, 419, 417 and 425. Other redundant paths would exist if the network were extended to more tiers and/or more nodes per tier.

Page 16

Please substitute the following paragraph for the paragraph beginning at line 7:

The locally hierarchical architecture described above greatly enhances security throughout the network since a response to an attack on one node will be controlled by another node which should respond correctly unless that node is simultaneously under attack, as well (prior faults throughout the network having been previously encapsulated and isolated). In such a case, a manager object at yet another node at a locally higher hierarchical level would control the active response, and so on, while establishing a

plurality of secure sessions and security domains (e.g. depicted by links 427, 415, 418, 425 of Figure 2~~Figure 3~~ between node 440 and node 450 as client and server and which may be defined by the user or automatically as an incident of routing or re-routing communications) over which control can be exercised through user transparent communications from a manager object at a node which remains trusted. A plurality of levels of trust can also be readily implemented for respective nodes and communicated throughout the network system or any desired portion thereof.

Page 19

Please substitute the following paragraph for the paragraph beginning at line 35:

It should also be understood that while the depiction of the network of Figure 4 is of planar topology insofar as the nodes which are depicted and a hierarchy of tiers is provided, only a locally hierarchical relationship between nodes is required and then only to the extent of ensuring an orderly relationship between manager objects and managed objects at different but connected nodes. Further, if it is desired to have a single node (which, if provided, is as fully secured as possible) for exercise of ultimate network security control and supervision at a higher hierarchical level than any other node, as alluded to above, the organization of the network system could be may triangular or pyramidal as depicted by chain line 310~~301~~.